DEPARTMENT OF CORRECTIONS
POLICIES AND PROCEDURES

Policy No. DOC 1.9.3	Subject: **OFFENDER ACCESS TO COMPUTERS**
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 5, plus attachment
Section 9: Information Systems	Revision Date: June 26, 2002 March 8, 2001; Dec. 1, 1999
Signature: /s/ Bill Slaughter	Effective Date: Dec. 1, 1996

I. POLICY:

It is the policy of the Department of Corrections to allow offenders controlled access to state owned computers. This access is allowed for training, legal research, educational purposes and as needed for work that offenders may perform in Department facilities/programs.

II. IMPLEMENTATION:

This policy was re-numbered without content change on June 26, 2002.

III. AUTHORITY:

2-15-112, MCA. Duties and Powers of Department Heads

2-15-114, MCA. Security responsibilities of departments for data and information technology resources

53-1-203, MCA. Powers and Duties of Department of Corrections

1-0250.00, MOM. Information Systems Security

Policy Memorandum from Department of Administration dated March 14, 1995.

IV. DEFINITIONS:

Computer Peripherals means any equipment that can be attached to a computer. Peripherals include, but are not limited to:

- printers;
- scanners;
- digital cameras; and
- zip drives.

Disks means computer disks including zip disks and compact disks (CD's), which can be used to transfer programs from computer to computer.

Freestanding Isolated Network means a group of computers networked only to each other. The freestanding isolated network will not have access to outside LANS, WANS, the Internet or Microsoft Outlook.

LAN (Local Area Network) means the Department of Corrections Local Area Network.

Offender means any individual in the custody of the Department of Corrections or its contractors.

Password means an alphanumeric combination of characters unique to individual users that allow access to a specific computer, network or computer system.

Stand-Alone Computer means a computer that is not attached to any network.

User ID is used generically to refer to logonID, loginID, userID, account, or any other term used to describe a user's rights and privileges on a computer, computer system or network.

VLAN means a network that is created specifically for offender use and is administered by the Department staff.

WAN (Wide Area Network) means the State of Montana Wide Area Network.

V. PROCEDURES:

A. Prohibitions

Under no circumstances will any offender be allowed:

1. Access to the internet

2. Access to e-mail or any other on-line service such as Microsoft Outlook
3. Supervisory or administrative access to file servers
4. Access to WANs
5. Access to non-offender LANs

B. Computer Labeling:

1. Offenders must only be allowed access to computers labeled Offender Use. All monitors and central processing units (CPU's) must be labeled in a conspicuous manner to ensure visual identity.

2. Facility/program staff computers must be labeled Staff Use on the face of the CPU and monitor.

3. A laminated card must be conspicuously attached to each Offender Use computer. The card must be signed and dated by the work area supervisor or computer staff and include all authorized programs allowed on the specific computer on which it is attached. In no case will offenders be allowed to save or maintain personal files on a state machine.

4. The work area supervisor, or designee, will inspect the Offender Use computers, at a minimum on a quarterly basis, to ensure that they are in compliance with the laminated card specifications. All inspections must be documented in writing.

C. Offender Access to Stand Alone Computers or Free Standing Isolated Networks:

1. An offender may be allowed access to stand alone computers and/or freestanding isolated networks at the discretion of the work area supervisor.

2. The computers must be labeled as outlined in Section B.

D. Offender access to V-LAN:

1. An offender may be allowed access to the offender VLAN, with written approval of the Department Computer Security Officer as well as the facility/program Warden/Superintendent/Administrator for work that the offender may perform in Department facilities/programs.

2. A request form for offender VLAN access (attachment A) must be completed by the requesting supervisor and forwarded to staff as outlined in Section D.

3. Once approved for VLAN access, offenders will have user ID numbers assigned to them, which must consist of a unique number determined by the facility/program.

4. When an offender leaves a job assignment, the work supervisor shall notify the Department Computer Security officer for removal of the offender from VLAN access.

E. Offender Access to LAN/WAN:

Under no circumstances are offenders to have access to LAN or WAN without approval from the Director, the State of Montana Computer Security Manager and Information Technologies Managers Council (ITMC).

F. Offender Access to Peripherals and Disks:

1. Each facility/program will ensure that offender access to peripherals is limited and closely supervised. Facilities/programs will develop specific policy regarding the use of all peripherals. In the case of scanners and digital cameras the supervisor must review and approve the project prior to allowing the offender access to the equipment.

2. Offenders may be allowed to use computer disks for appropriate work related assignments and educational programs, in coordination with the computer security officer and area supervisor. In

no case will offenders be allowed to move disks from their assigned work area to another area without staff approval. Possession of disks in their living area or use of disks for personal needs is strictly prohibited. Facilities/programs may label disks that are used by offenders as another level of security.

VI. CLOSING:

Questions concerning this policy should be directed to the Department Information Technology Bureau Chief.

OFFENDER ACCESS TO DOC COMPUTER VLAN REQUEST FORM

This form will be used for all requests for offender access to the DOC computer Virtual Local Area Network (VLAN). Please complete and route this request form in the order of the following sections.

The following portion to be completed and signed by the work supervisor:

DOC Division: _____

Offender Work Location: _____

Offender Name: _____ DOC ID #: _____

Justification for VLAN request: _____

_____

_____

Work Supervisor Printed Name: _____

Work Supervisor Signature: _____ Date: _____

Program Manager/Director Signature: _____ Date: _____

The following portion to be completed by the appropriate Division Administrator, Warden or designee.

Approved: ☐ Disapproved: ☐ Date: _____

Comments: _____

_____

_____

Printed Name: _____ Signature: _____

The following section to be completed by the DOC Information Technology Bureau:

☐ Approved: ☐ Disapproved: Date: _____

Comments: _____

_____

_____

Printed Name: _____ Signature: _____

Printed Name: _____ Signature: _____

UserID # Assigned: _____ Effective Date: _____

Copies go to originating work location, Facility Security Manager/Major, and the DOC Information Technology Bureau upon completion of all sections above.